

§ 1311.10

(b) These standards are available from the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899-8930, (301) 975-6478 or TTY (301) 975-8295, inquiries@nist.gov, and are available at <http://csrc.nist.gov/>. The following standards are incorporated by reference:

(1) Federal Information Processing Standard Publication (FIPS PUB) 140-2, Change Notices (12-03-2002), Security Requirements for Cryptographic Modules, May 25, 2001 (FIPS 140-2) including Annexes A through D; incorporation by reference approved for §§ 1311.30(b), 1311.55(b), 1311.115(b), 1311.120(b), 1311.205(b).

(i) *Annex A*: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, September 23, 2004.

(ii) *Annex B*: Approved Protection Profiles for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, November 4, 2004.

(iii) *Annex C*: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, January 31, 2005.

(iv) *Annex D*: Approved Key Establishment Techniques for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, February 23, 2004.

(2) Federal Information Processing Standard Publication (FIPS PUB) 180-2, Secure Hash Standard, August 1, 2002, as amended by change notice 1, February 25, 2004 (FIPS 180-2); incorporation by reference approved for §§ 1311.30(b) and 1311.55(b).

(3) Federal Information Processing Standard Publication (FIPS PUB) 180-3, Secure Hash Standard (SHS), October 2008 (FIPS 180-3); incorporation by reference approved for §§ 1311.120(b) and 1311.205(b).

(4) Federal Information Processing Standard Publication (FIPS PUB) 186-2, Digital Signature Standard, January 27, 2000, as amended by Change Notice 1, October 5, 2001 (FIPS 186-2); incorporation by reference approved for §§ 1311.30(b) and 1311.55(b).

(5) Federal Information Processing Standard Publication (FIPS PUB) 186-3, Digital Signature Standard (DSS),

21 CFR Ch. II (4-1-21 Edition)

June 2009 (FIPS 186-3); incorporation by reference approved for §§ 1311.120(b), 1311.205(b), and 1311.210(c).

(6) Draft NIST Special Publication 800-63-1, Electronic Authentication Guideline, December 8, 2008 (NIST SP 800-63-1); Burr, W. et al.; incorporation by reference approved for § 1311.105(a).

(7) NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007 (NIST SP 800-76-1); Wilson, C. et al.; incorporation by reference approved for § 1311.116(d).

[75 FR 16310, Mar. 31, 2010]

Subpart B—Obtaining and Using Digital Certificates for Electronic Orders

§ 1311.10 Eligibility to obtain a CSOS digital certificate.

The following persons are eligible to obtain a CSOS digital certificate from the DEA Certification Authority to sign electronic orders for controlled substances.

(a) The person who signed the most recent DEA registration application or renewal application and a person authorized to sign a registration application.

(b) A person granted power of attorney by a DEA registrant to sign orders for one or more schedules of controlled substances.

§ 1311.15 Limitations on CSOS digital certificates.

(a) A CSOS digital certificate issued by the DEA Certification Authority will authorize the certificate holder to sign orders for only those schedules of controlled substances covered by the registration under which the certificate is issued.

(b) When a registrant, in a power of attorney letter, limits a certificate applicant to a subset of the registrant's authorized schedules, the registrant is responsible for ensuring that the certificate holder signs orders only for that subset of schedules.

§ 1311.20 Coordinators for CSOS digital certificate holders.

(a) Each registrant, regardless of number of digital certificates issued,

must designate one or more responsible persons to serve as that registrant's CSOS coordinator regarding issues pertaining to issuance of, revocation of, and changes to digital certificates issued under that registrant's DEA registration. While the coordinator will be the main point of contact between one or more DEA registered locations and the CSOS Certification Authority, all digital certificate activities are the responsibility of the registrant with whom the digital certificate is associated. Even when an individual registrant, *i.e.*, an individual practitioner, is applying for a digital certificate to order controlled substances a CSOS Coordinator must be designated; though in such a case, the individual practitioner may also serve as the coordinator.

(b) Once designated, coordinators must identify themselves, on a one-time basis, to the Certification Authority. If a designated coordinator changes, the Certification Authority must be notified of the change and the new responsibilities assumed by each of the registrant's coordinators, if applicable. Coordinators must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.

(2) A copy of each current DEA Certificate of Registration (DEA form 223) for each registered location for which the coordinator will be responsible or, if the applicant (or their employer) has not been issued a DEA registration, a copy of each application for registration of the applicant or the applicant's employer.

(3) The applicant must have the completed application notarized and forward the completed application and accompanying documentation to the DEA Certification Authority.

(c) Coordinators will communicate with the Certification Authority regarding digital certificate applications, renewals and revocations. For applicants applying for a digital certificate from the DEA Certification Authority, and for applicants applying for a power of attorney digital certificate for a DEA registrant, the registrant's Coordinator

must verify the applicant's identity, review the application package, and submit the completed package to the Certification Authority.

§ 1311.25 Requirements for obtaining a CSOS digital certificate.

(a) To obtain a certificate to use for signing electronic orders for controlled substances, a registrant or person with power of attorney for a registrant must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.

(2) A current listing of DEA registrations for which the individual has authority to sign controlled substances orders.

(3) A copy of the power of attorney from the registrant, if applicable.

(4) An acknowledgment that the applicant has read and understands the Subscriber Agreement and agrees to the statement of subscriber obligations that DEA provides.

(b) The applicant must provide the completed application to the registrant's coordinator for CSOS digital certificate holders who will review the application and submit the completed application and accompanying documentation to the DEA Certification Authority.

(c) When the Certification Authority approves the application, it will send the applicant a one-time use reference number and access code, via separate channels, and information on how to use them. Using this information, the applicant must then electronically submit a request for certification of the public digital signature key. After the request is approved, the Certification Authority will provide the applicant with the signed public key certificate.

(d) Once the applicant has generated the key pair, the Certification Authority must prove that the user has possession of the key. For public keys, the corresponding private key must be used to sign the certificate request. Verification of the signature using the public key in the request will serve as proof of possession of the private key.